4.5 NETWORK MENU

The Network menu provides utilities to manage the general configuration of individual workstations as well as the local LAN and to manage the interface between the workstations and the LAN. The Network menu provides the following options:

Change Machine ID
To change the name of a machine on a network. (Section 4.5.1)

Set System Time
To set the time on the workstation to match that of the comms server. (Section 4.5.2)

Set WAN UID
To set the wide-area network (WAN) unique ID (UID). (Section 4.5.3)

Set WAN DDN Timeout
To allow the system administrator to set a time-out period for DDN network operations. (Section 4.5.4)

Config DDN Host Table
To create a Data Defense Network (DDN) host table to describe the entire WAN. (Section 4.5.5)

Set NIPS TDBM Host
To designate a workstation where a user can perform Naval Intelligence Processing System (NIPS) track updates. (Section 4.5.6)

Edit Local Hosts
To add or delete a list of hosts that can be accessed from a user's machine. (Section 4.5.7)

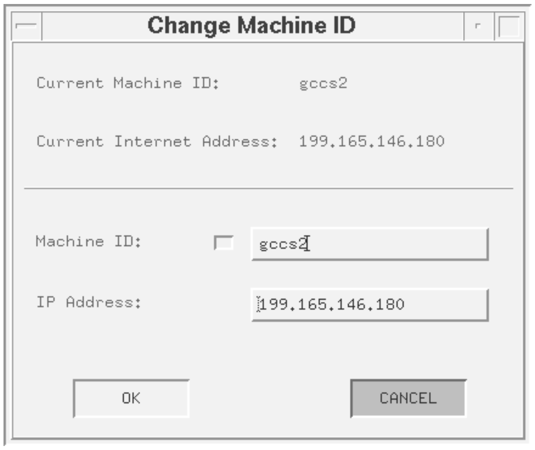
System Configuration
To set the list of available hosts for the local machine. (Section 4.5.8)

4.5.1 CHANGE MACHINE ID

The CHANGE MACHINE UNIQUE ID option changes the name of a machine on a network.

WARNING: The machine will reboot when you use this utility. If circumstances prevent you from rebooting the machine, do not use this option.

Each workstation on an Ethernet must have its own unique network address. This address is set when the system is installed and is associated with a symbolic name. The network does not permit two machines with the same name. Select CHANGE MACHINE UNIQUE ID to view the Change Machine ID window:



Change Machine ID

Current Machine ID: gccs2

Current Internet Address: 199.165.146.180

Machine ID: □ gccs2

IP Address: 199.165.146.180

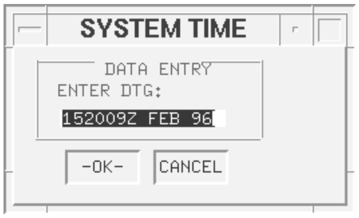
Figure 4-16 Change Machine ID Window

1. Click the up or down arrow to scroll through the list of machine names.
2. After selecting the machine name, click OK to complete the change. (If the name is already used on the LAN, an error message prompts for another name.)
3. After the name is accepted, a warning window alerts you that the system will reboot.
4. Click OK to reboot the machine or CANCEL to prevent the reboot. The reboot is required to change the name (ID) of the machine.
5. After the reboot process is complete, you are returned to the Login window.

4.5.2 SET SYSTEM TIME

The JMCIS comms processor must have the correct ZULU time or track reports may fail to process. JMCIS will not process track reports "in the future" (i.e., with time/pos lines ahead of the JMCIS clock). To avoid failed track reports, set the JMCIS system time as follows:

1. From the NETWORK menu, select the SET SYSTEM TIME option. The SYSTEM TIME window appears.



ENTER DTG:
152009Z FEB 96

Figure 4-17 SYSTEM TIME Window

2. Enter the correct ZULU time in DDHHMMZ MON YR format.
3. Click OK to set the JMCIS system time.

4.5.3 SET WAN UID

A unique ID (UID) is critical to the integrity of the Data Defense Network's (DDN) contact database. Each wide-area network (WAN) site is assigned a unique address. This address and the corresponding unique name of each system on the network are used by the system to create a UID for each contact that enters the system. Note that the UID is displayed in the track edit window in a non-edit field, and therefore it cannot be altered by the operator.

The UID is formatted as XXX, where XXX is a three character WAN DDN UID, or station identifier, assigned to your particular JMCIS system. The three-character ID marks tracks added to the DDN from your system.

The UID code you provide using this window ensures that tracks added to the database from two different terminals on the WAN are uniquely identified *even if they are added at precisely the same time*. While the time/date stamps of the two tracks may be identical, the first three characters of the UID are different since the contacts were added at different stations. Thus, the two parts of the UID work in conjunction to uniquely identify every track added to the track database.

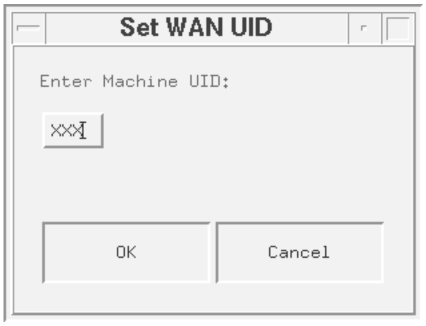
Each track is assigned a UID. However, the UID may or may not be used depending on your system's operating mode. For example, if UID CORRELATION MODE is selected in the EDIT FOTC CONFIGURATION window, any contact database information received over the DDN is processed according to its WAN DDN UID before any other type of correlation is done. This first pass through the database looks solely for exact UID matches to the incoming track. UID matches are updated directly regardless of any other considerations such as attribute mismatches or geofeasibility concerns. The track's history is updated and, in the event of mismatched attribute data, existing attribute information is replaced by that of the incoming track. If no match is found in the track database, normal attribute correlation is then performed.

In general, ashore installations operate in FOTC Non-participant or in UID Correlation mode, while afloat sites select from FOTC Coordinator, FOTC Participant, or FOTC Non-participant modes.

Warning: For Ashore Sites Only

Using UID Correlation mode without a valid WAN DDN UID can cause serious database problems. Do not select UID Correlation mode before you have entered a valid WAN DDN UID.

From the NETWORK menu, select the SET WAN DDN UID option to set your system's WAN DDN UID. The SET WAN UID window appears.



Enter Machine UID: XXX

Figure 4-18 Set WAN UID Window

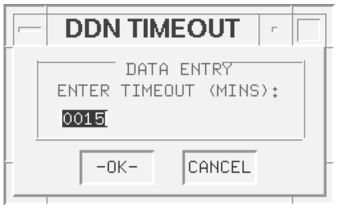
Enter your assigned UID into the highlighted field, then press [Return]. (Or, if you prefer, enter the UID and click OK.) If you decide not to change the default UID, click CANCEL.

4.5.4 SET WAN DDN TIMEOUT

This option allows the system administrator to set a timeout period for DDN network operations. The timeout period begins after the DDN channel is started.

If a requested connection to a remote host fails, or if the receipt timeout period expires, a DDN STATUS UNCERTAIN warning is put in the alert log. (If the DDN TIMEOUT knob in the SCREEN ALERT FILTER window is selected, a window also appears on the tactical display.)

Select the SET WAN DDN TIMEOUT INTERVAL option to set your system timeout. The DDN TIMEOUT window appears:



ENTER TIMEOUT (MINS): 0015

Figure 4-19 DDN TIMEOUT Window

Timeout values must be between 1 and 3600 minutes. The default value is 15 minutes (0015). Enter the desired timeout length (in minutes) into the highlighted field, and click OK. If you decide not to change the default value, click CANCEL.

4.5.5 CONFIG DDN HOST TABLE

Warning: This option is for use only by hub sites.

If you are a hub site and you need to reload the JMCIS software for any reason, make sure to restore the data for this option using your tape backup of the DDN host table after the basic installation has been completed. If you do not have a tape backup of the DDN host table, follow the steps listed below to recreate the DDN host table.

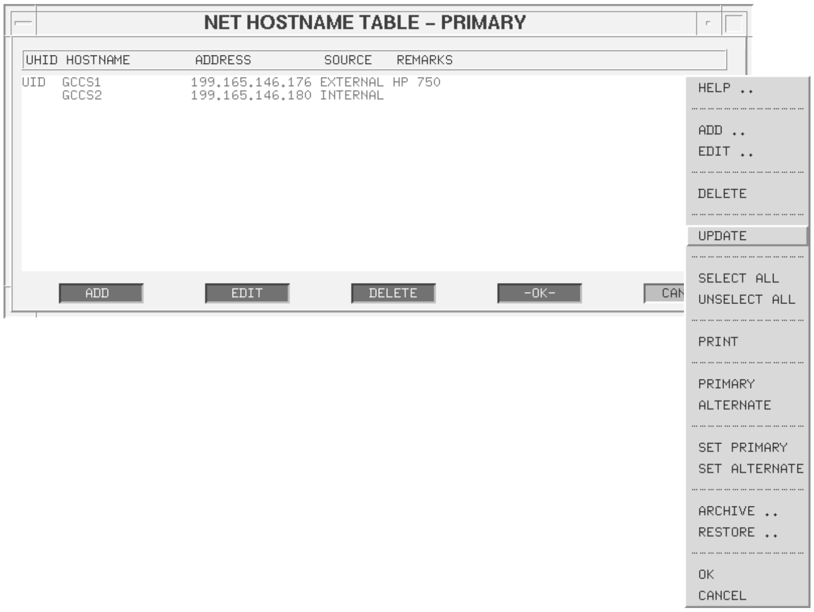
The Data Defense Network (DDN) host table describes the entire wide-area network (WAN). A “generic” host table is established in the operating system during installation. The system administrator must edit a copy of the generic table so that each site with which you intend to communicate given a UHID. Most sites communicate with only a few other sites, so unedited host table entries should be deleted.

Note: Sometimes a site is designated to be a backup for a centralized communications site. The backup site must be prepared to quickly go on-line in case the system at the primary site, or hub, goes down. The CONFIGURE DDN HOST TABLE option provides a means to store two separate host tables, allowing you to quickly go on-line as a hub. If your site serves as a backup communications hub, you should set up the two host tables as follows:

- Primary: lists the sites you need for normal communications.
- Alternate: lists the sites used by the hub that you are backing up.

The easiest way to configure these tables is to set up the alternate table *first*, then set up the primary table, which is usually a subset of the sites listed in the alternate table.

Once the tables have been set up, it is easy to switch between the two. The current table appears as part of the NET HOSTNAME TABLE window title. If the window title reads NET HOSTNAME TABLE–ALTERNATE, select PRIMARY from the window's pop-up menu to view the sites you use under normal operating circumstances. If the window title reads NET HOSTNAME TABLE–PRIMARY, select ALTERNATE from the window's pop-up menu to see the entries used by the hub you are backing up.



```
UHID HOSTNAME      ADDRESS          SOURCE   REMARKS
UID  GCCS1         199.165.146.176  EXTERNAL HP 750
     GCCS2         199.165.146.180  INTERNAL
```

Figure 4-20 NET HOSTNAME TABLE– PRIMARY Window, with pop-up menu

The following steps describe how to set up the DDN host table.

1. Select CONFIGURE DDN HOST TABLE from the SYSTEM ADMINISTRATION window.
2. Select UPDATE from the pop-up window to read a copy of the host table from the operating system. The entire file is read in from the operating system.
3. If your site serves as backup for a hub site, select SET ALTERNATE from the pop-up menu. *If your site is not a hub backup*, skip to Step 4.
4. Select the first site in the default list with which you will routinely communicate.

5. Click EDIT to bring up the EDIT HOSTNAME window. Fill in the site's UHID, hostname, address, and any desired remarks in the appropriate fields.
6. Note that the default for each site is *internal*. If the site is external, make sure to click the checkbox so it appears empty. An empty checkbox means that the site is *external*.
7. Click OK.
8. Repeat Step 4 through Step 7 for each of the remaining sites with which you communicate.
9. Choose the SELECT ALL option from the pop-up menu.
10. Deselect all the sites you just edited; they appear at the top of the list.
11. Click DELETE to remove all the highlighted sites since they have not been assigned a UID.

Note: Perform Step 12 through Step 15 only if your site is a hub backup. Otherwise, skip to Step 16.

12. Select SET PRIMARY from the CONFIGURE DDN HOST TABLE window pop-up menu.
13. Highlight and delete any sites that you will not communicate with under normal operating conditions.
14. If you need to add any sites to the primary list, click ADD. Enter the site's UHID, hostname, address, and any desired remarks in the appropriate fields. If the site is external, make sure to click the checkbox so it appears empty.
15. When the list contains all sites you will communicate with under normal operating conditions, select SET PRIMARY from the pop-up menu.
16. Archive the host table to the clipboard, then make a tape backup of the host table data. *If your site serves as a hub backup, make tape backups of both the primary and alternate host tables.* Store the backup tape in a safe place so that you can recover quickly in the event your host tables become corrupted.

    DDN, in general:

    - Click ADD to add a new site to the DDN hostname table.
    - Click EDIT to edit the UHID, hostname, address, remarks, or internal/external flag of an existing site.
    - Click DELETE to remove an existing site from the list.
    - Click CANCEL to close the NET HOSTNAME TABLE window without saving your changes.

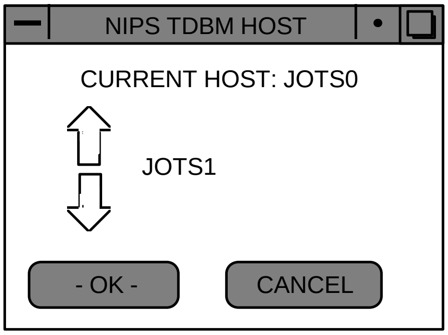
- Click OK to store the new configuration.

4.5.6 SET NIPS TDBM HOST

Use this option to designate the workstation where a user can perform Naval Intelligence Processing System (NIPS) track updates.

- The CP (usually gccs1) should *not* be a NIPS Tdbm host.
- UB tracks can be associated with (or disassociated from) NIPS tracks.
- When updates are received on associated tracks, the NIPS Tdbm automatically updates the NIPS tactical tables.

To access this window: NETWORK menu **:** SET NIPS TDBM HOST option **:** NIPS TDBM HOST window (Figure 5-18).



CURRENT HOST: JOTS0

JOTS1

Figure 5-18 NIPS Tdbm Host Window

1. Click on the arrows until the workstation connected to the NIPS database appears in the window.
2. Click OK to select the host workstation, or click CANCEL to discard the change.

4.5.7 EDIT LOCAL HOSTS

This option lists the machines that can be accessed from a user's machine. Use this option to:

- Add or delete machines from the list
- Modify machine information, such as name, IP address, or aliases.

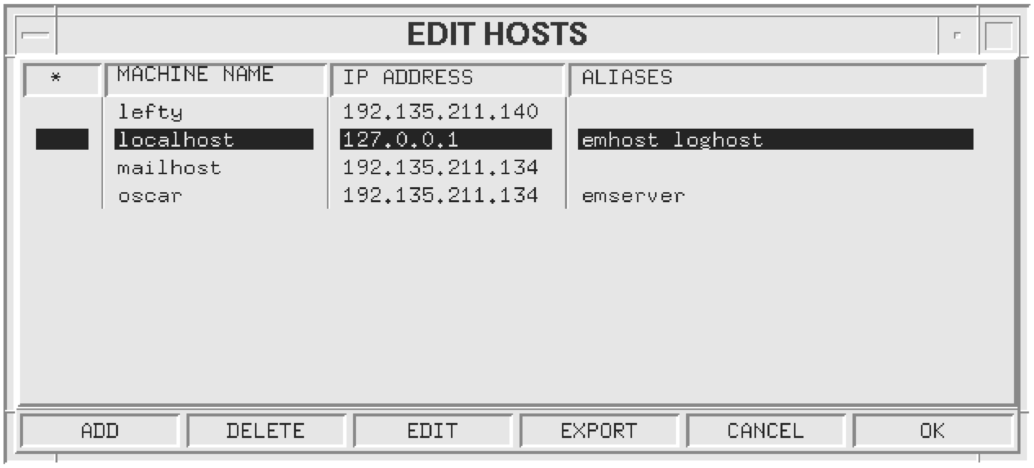
Important considerations for modifying host information such as creating user-defined machine names:

- Change information (names, IP addresses, and aliases) *after* all machines are installed, but *before* the system is used.

- Make changes *first* on the CP for the LAN.
- All changes must be repeated *exactly the same* on each LAN machine– defining the same information, in the same order, on each machine.

To modify information, complete the following tasks on each machine.

To access this window: NETWORK pull-down menu **:** EDIT LOCAL HOST option **:** EDIT HOSTS window (Figure 4-21).



*	MACHINE NAME	IP ADDRESS	ALIASES
	lefty	192.135.211.140	
	localhost	127.0.0.1	emhost loghost
	mailhost	192.135.211.134	
	oscar	192.135.211.134	emserver

Figure 4-21 Edit Hosts Window

About the EDIT HOST Window:

Two steps are required to add, edit, or delete a machine.

1. After completing the selected action (add, delete, or edit), the machine remains in the EDIT HOSTS window labeled with A (add), M (modify), or D (delete), in the * column. The machines will continue to have this designation until such time as you exit the window. If you access the window again, the A, M, or D designations are removed.
2. Click OK to accept the changes to the machine. Click CANCEL to discard the changes.

EDIT HOSTS Window Buttons:

ADD– a machine to the LAN. (Described in *Add a Machine*.)

DELETE– a machine from the LAN.

1. Highlight a machine in the list.

2. Click DELETE.
3. Click YES in the warning window to confirm the delete, or NO to cancel.

EDIT– a machine name.

1. Highlight one machine name and click EDIT to open the EDIT MACHINE window.
2. The EDIT MACHINE window functions the same as the ADD MACHINE window. (Described in *Add a Machine*.)

EXPORT– machine information to other workstations on the LAN. (Not currently implemented.)

CANCEL– close the window without saving changes.

OK– close the window and save changes.

EDIT LOCAL HOST Window Fields

*****

A (add), D (delete), or M (modify) indicate pending changes made to the machine. T indicates a trusted machine.

A trusted machine can be accessed from another machine on the same LAN. For example, a trusted machine can be used to access a tape drive for a remote installation if your local machine does not have a tape drive attached to it.

MACHINE NAME

Name of the machine. This can be system-defined (gccs1, gccs2, etc.) or user-defined.

IP ADDRESS

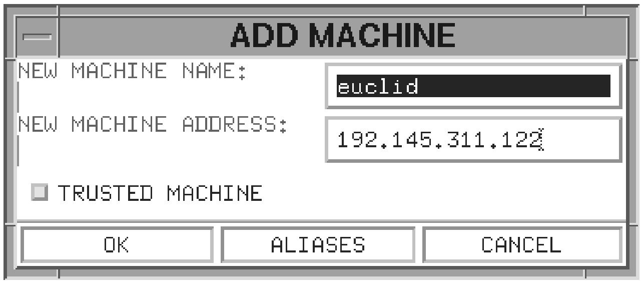
Unique Internet protocol address.

ALIASES

List of other names by which a machine is also known.

4.5.7.1 Add a Machine

Use this option to add a machine to the LAN.



NEW MACHINE NAME: euclid

NEW MACHINE ADDRESS: 192.145.311.122

□ TRUSTED MACHINE

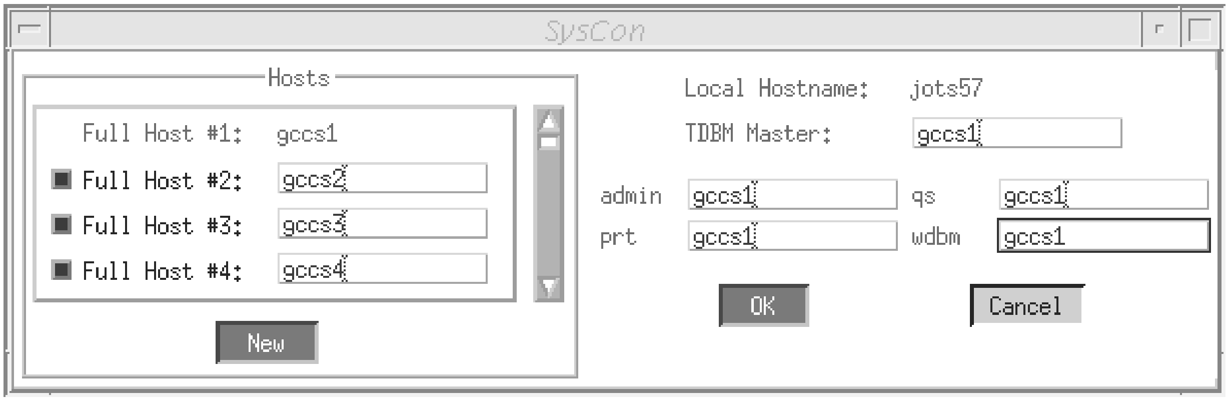
Figure 4-22 Add Machine Window

1. From the EDIT HOSTS window, click ADD to open ADD MACHINE window (Figure 4-22).
2. Enter the machine name in the NEW MACHINE NAME field.
3. Enter the machine IP address in the NEW MACHINE ADDRESS field.
4. Toggle TRUSTED MACHINE checkbox ON to define the new machine as a trusted machine.
5. To add or delete aliases for a machine:
    - Click ALIASES to open the ALIASES window.
    - ADD or DELETE one or more aliases. (Allowable characters are the same as for MACHINE NAME.)
    - Press RETURN to accept a new alias.
    - Click OK to close the ALIASES window and save changes.
6. Click OK to mark the machine as an addition to the list of available machines on the LAN, or click CANCEL to discard changes.

4.5.8 SYSTEM CONFIGURATION

In order for a local workstation running GCCS software to be fully operational within the LAN, a list of hosts in the LAN must be configured on the local machine. The SysCon window provides an interface to set the host names in the resource files that are required to run GCCS software.

To view the current SysCon window, select System Configuration from the Network menu. The SysCon window appears.



Full Host #1: gccs1

■ Full Host #2: gccs2

■ Full Host #3: gccs3

■ Full Host #4: gccs4

Local Hostname: jots57

TDBM Master: gccs1

admin gccs1 qs gccs1

prt gccs1 wdbm gccs1

Figure 4-23 SysCon Window

Two types of hosts may be set using the SysCon window: Full hosts and Printer hosts. Full hosts are other hosts on the network, including the administrative, broadcast, and pcm hosts. Printer hosts are print servers or printer clients for the various printers that may be enabled from the workstation. A Full host may also be used as a printer server. The Full hosts defined in this function are provided as hosts for various functions in GCCS, including available MACHINE options on various communications interfaces.

The SysCon window initially displays a generic listing of 30 potential full hosts and 5 printer hosts in a Hosts box on one side of the window (defaults to jots1 through jots30 and milan 1 through milan 5). Note that the first entry in this list of hosts is non-editable and reflects your workstation’s TDBM Master entry, set by entering the TDBM Master hostname in the TDBM Master field to the right of the Hosts box.

To the right of the Hosts box in the SysCon window, several fields allow you to define specific hosts which provide specific services and networking functions in conjunction with your workstation. The Local Hostname field is a non-editable field that displays your workstation’s hostname.

Warning: When *moving* a TDBM Master from one machine to another on a functioning system (i.e., *after* initial installation), you must take care never to have more than one TDBM Master operating simultaneously. Should this happen, it could cause large data loss, as two masters would be competing over use of the same global data. To avoid this condition, ***ensure that you reconfigure the existing TDBM Master before you reconfigure the new TDBM master*** (i.e., if Machine A is the old (current) TDBM Master, and Machine B is the new TDBM Master, first make Machine A a slave to Machine B, and then make Machine B the TDBM Master.

The TDBM Master: field allows you to set the TDBM Master hostname. This field also determines the setting for the Full Host #1 in the Hosts box. Several other fields allow you to define other server hosts (broadcast, pcm, etc.) related to the workstation.